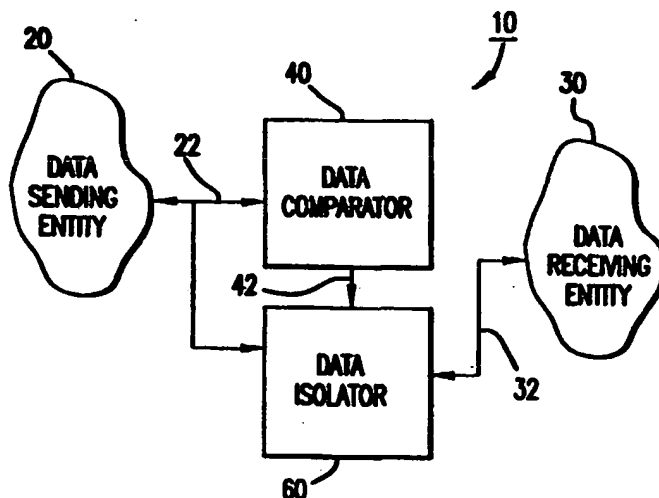




## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification <sup>6</sup> : <b>H04L 12/22, 9/00</b>	<b>A1</b>	(11) International Publication Number: <b>WO 99/29066</b> (43) International Publication Date: 10 June 1999 (10.06.99)
(21) International Application Number: <b>PCT/US98/25579</b> (22) International Filing Date: 3 December 1998 (03.12.98) (30) Priority Data: 08/984,608        3 December 1997 (03.12.97)        US (71) Applicant: RVT TECHNOLOGIES, INC. [US/US]; Suite 109, 4485 Highway 29, Lilburn, GA 30047 (US). (72) Inventor: MANN, Steven, D.; 20 Hearthstone Drive, Stock- bridge, GA 30281 (US). (74) Agents: ROSENBERG, Sumner, C. et al.; Needle & Rosenberg, P.C., 127 Peachtree Street, N.E., Atlanta, GA 30303 (US).	(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CP, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).  Published With international search report.	

(54) Title: METHOD AND APPARATUS FOR ISOLATING AN ENCRYPTED COMPUTER SYSTEM UPON DETECTION OF VIRUSES AND SIMILAR DATA



## (57) Abstract

A method and apparatus for isolating a data receiving entity (30) from a data sending entity (20) include a first data channel (22), coupled to the data sending entity (20), and a second data channel (32), coupled to the data receiving entity. A data encryption chip decrypts data received from the data sending entity (20) and encrypts data sent to the data sending entity (20). A processor is programmed to compare a plurality of data words received from the first data channel to at least one data word characteristic of a data virus (40) and to assert a control signal (42) when a data word received from the first data channel corresponds to a data word characteristic of a data virus. An optical isolator (60) is capable of isolating the first data channel from the second data channel when the processor detects a data virus.

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakhstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

**METHOD AND APPARATUS FOR ISOLATING AN ENCRYPTED  
COMPUTER SYSTEM UPON DETECTION OF VIRUSES AND SIMILAR  
DATA**

5                   **CROSS-REFERENCE TO RELATED APPLICATION**

This is a continuation-in-part of my copending applications filed October 22, 1997, Serial No.: 08/955,912, the disclosure for which is incorporated herein by reference.

10

**BACKGROUND OF THE INVENTION**

1. Field of the Invention:

15           This invention relates to computer systems. More particularly, this invention relates to a method and apparatus for isolating a computer system upon detection of a virus and similar data.

2. The Prior Art:

20

Recently, transmission of data viruses over the Internet has become a serious concern for Internet users. To reduce the concern, several methods are used to isolate computers from the Internet while the users are in local mode. However, when users of such methods are in a connected mode, they become  
25 prey to any virus that they may unwittingly download.

Computer virus scanners are common and can be used to detect a virus once it is downloaded. However, such scanners cannot prevent the virus from  
30 being downloaded. They can only aid in the identification of a virus once it has already infected the user's computer.

Data security involving data networks is also an important concern. Many systems encrypt data sent over a network. However, no existing systems provide both data encryption/decryption and virus detection, thereby ensuring complete data security for transmitted and received data.

5

Nowhere does the prior art disclose a method or apparatus for detecting a virus as it is being received from a network and isolating the user's computer from the Internet when an incoming virus is detected.

10

## SUMMARY OF THE INVENTION

The above-noted disadvantages of the prior art are overcome by the present invention, which in one aspect is an apparatus for isolating a data receiving entity from a data sending entity. A first data channel is coupled to the data sending entity and a second data channel is coupled to the data receiving entity. A circuit facilitates encryption and decryption of the data being received from and transmitted to the data sending entity. A processor is operationally coupled to the first data channel and detects a data virus received from the first data channel. An isolation circuit that is responsive to the processor couples the first data channel to the second data channel when the processor does not detect a data virus and isolates the first data channel from the second data channel when the processor detects a data virus.

15

20

25

In another aspect, the invention includes a first data channel coupled to the data sending entity and a second data channel coupled to the data receiving entity. A data encryption chip is operationally coupled to the first data channel. A processor, operationally coupled to the data encryption chip and that is programmed to compare a plurality of data words received from the first data channel to at least one data word characteristic of a data virus asserts

a control signal when a data word received from the first data channel corresponds to a data word characteristic of a data virus. A memory, that is operationally coupled to the processor, stores at least one data word characteristic of a data virus. The memory presents to the processor at least one data word characteristic of a data virus and an input buffer stores data received by the processor from the first data channel. An optical isolator, coupled to the first data channel and the second data channel and having an enable signal input, is capable of isolating the first data channel from the second data channel when the enable signal input is not asserted and is also capable of placing the first data channel and the second data channel in optical communication with each other when the enable signal input is asserted. A controllable power supply that is responsive to the control signal from the processor is coupled to the enable signal input of the optical isolator. The power supply asserts the enable signal when the control signal is not asserted and does not assert the enable signal when the control signal is asserted, thereby causing the optical isolator to isolate the first data channel from the second data channel.

In yet another aspect, the invention is a method for isolating data receiving entity from a data sending entity. When a data virus received from the data sending entity is detected, the data sending entity is isolated from the data receiving entity.

An advantage of the invention is that it prevents a data receiving entity, such as a computer, from receiving a virus from a data sending entity, such as a computer network.

A further advantage of the invention is that it isolates the data sending entity from the data receiving entity without disrupting normal operation of either entity.

5           A further advantage of the invention is that it allows for encryption and decryption of communicated data.

10           These and other advantages will become apparent from the following description of the preferred embodiment taken in conjunction with the following drawings, although variations and modifications may be effected without departing from the spirit and scope of the novel concepts of the disclosure.

#### **BRIEF DESCRIPTION OF THE FIGURES OF THE DRAWINGS**

15           **FIG. 1** is a simplified schematic diagram of the invention.

**FIG. 2** is a detailed schematic diagram of the invention.

20           **FIG. 3** is a detailed schematic diagram of an embodiment of the invention that includes data encryption.

#### **DETAILED DESCRIPTION OF THE INVENTION**

25           A preferred embodiment of the invention is now described in detail. Referring to the drawings, like numbers indicate like parts throughout the views. As used in the description herein and throughout the claims that follow, "a," "an," and "the" includes plural reference unless the context clearly dictates otherwise. Also, as used in the description herein and throughout the

claims that follow, the meaning of "in" includes "in" and "on" unless the context clearly dictates otherwise.

As shown in FIG. 1, the apparatus 10 of the invention evaluates data  
5 received from a data sending entity 20, such as the Internet, by a data  
receiving entity 30, such as a personal computer or even a local area network.  
The data is received via a first data channel 22 coupled to the data sending  
entity 20 and a second data channel 32 coupled to the data receiving entity. A  
data comparator 40 is operationally coupled to the first data channel 22 and is  
10 used to detect data viruses received from the first data channel 22. When a  
virus is detected, a data isolator 60, that is responsive to a control signal 42  
from the data comparator 40, isolates the first data channel 22 from the second  
data channel 32. Thus, viruses are detected and prevented from being received  
by the data receiving entity 30.

15 As shown in FIG. 2, the apparatus 10 of one preferred embodiment of  
the invention interfaces with a peripheral control interface (PCI) 12 of a data  
receiving entity 30, such as a personal computer, to provide isolation from a  
data sending entity 20, such as the Internet. The data sending entity 20 is  
20 connected to an input interface 24, such as a standard PBX interface, via a first  
data channel 22. The data stream received by the input interface 24 is  
demodulated using a demodulator circuit 26 so as to conform to the data  
format of the data receiving entity 30.

25 The data stream is then fed into the data comparator 40. In the  
comparator circuit 40, a UART chip 46 formats the incoming serial data into  
parallel data words and a processor 44, such as a PCI host controller, using an  
asynchronous transfer mode segmentation and reassembly, compares the  
parallel data with known virus signatures stored in a memory 48, such as an

EEPROM. The processor 44, which is controlled by a control memory 50, buffers data from the UART chip 46 in a memory chip 52 as it awaits virus scanning analysis.

5           After the processor 44 has analyzed an incoming word, it is then sent to the data isolator 60 for eventual transfer to the data receiving entity 30. The data isolator 60 comprises an optical isolator 62 that is driven by a power enable signal 66 received from a power supply conditioning ISO drive 64. The power supply conditioning ISO drive 64 receives power from a power up  
10 control logic circuit 54 which receives power from a power line 74 in the PCI bus 12.

          If no virus is found, the data stream is transferred through the optical isolator 62 to a modulation level shifting circuit 68, that conditions the data for  
15 receipt by the data receiving entity 30, to a modem interface 34. The modem interface 34 provides protocol matching to the input interface 24 and sends the data to the data receiving entity 30.

          When a virus is detected in the incoming data stream, a control line 42  
20 from the processor 44 causes the power up control logic circuit 54 to cause the power supply conditioning ISO drive 64 to cut off power to the optical isolator 62, thereby causing the optical isolator 62 to prevent passage of data therethrough. A modem standby circuit 36 then takes over and simulates protocol exchanges with the input interface 24, thereby preventing an  
25 abnormal disconnect.

          During power-up, the processor 40 runs the system through a self checking routine. If any system abnormalities are detected, an interrupt line

70 is asserted. The interrupt line 70 passes through an optical isolator 14 to ensure unidirectional data transmission to the PCI bus 12.

5       The power up control logic circuit 54 also performs a self check. a battery reference 56 is compared to the value on the incoming power line 74 from the PCI bus 12, and if the system is improperly powered, an interrupt line 72 is asserted. The interrupt line 72 is also passed through an optical isolator 16 that ensures that the interrupt line 72 is unidirectional to the PCI bus 12.

10       As shown in FIG. 3, an embodiment of the invention 100 that includes data encryption/decryption includes a data cipher processor 180 to encrypt/decrypt communicated data. The cipher processor 180 could be a TUNDRA CA95C68, or other encryption chip. In this embodiment, data is received from the network by a network interface 122, which would be a  
15       standard RJ45 connection, or similar network interface. A data format chip 146 formats the data for the cipher processor 180, which provides decrypted data to the screening environment processor 144. The screening environment processor 144, which provides virus detection, could comprise a digital signal processing (DSP) chip, such as an ADSP-2181 and is serviced by a memory  
20       150. A micro-controller 134 is provided to control the data processing elements in the invention 100, sends control information to the host computer's PCI bus 112 and initiates communication handshaking. The screening environment processor 144 provides a control signal to an opto-isolator bank 162, which isolates the host personal computer 130 from the  
25       network interface 122 upon detection of a virus.

      Data from the opto-isolator bank 162 is conditioned by a network interface card 132 to make it suitable for the personal computer 130. An opto drive 164 conditions power to the opto-isolator bank 162.

A power-up conditioner 154 taps power from the PCI bus 112 and provides power to the opto-drive 164. The power-up conditioner 154 also sends status signals to the PCI bus 112 through a pair of opto-isolators 114, 116 used to maintain unidirectional data transfer. A battery reference 156 provides the power-up conditioner 154 with a voltage reference, to facilitate self checking functions.

The above described embodiment is given as an illustrative example only. It will be readily appreciated that many deviations may be made from the specific embodiment disclosed in this specification without departing from the invention. Accordingly, the scope of the invention is to be determined by the claims below rather than being limited to the specifically described embodiment above.

**CLAIMS****What is claimed is:**

1. An apparatus for isolating data receiving entity from a data sending entity, comprising:
  - a. a first data channel, coupled to the data sending entity;
  - b. a second data channel, coupled to the data receiving entity;
  - c. means, operationally coupled to the first data channel, for detecting a data virus received from the first data channel;
  - d. means, responsive to the detecting means, for coupling the first data channel to the second data channel when the detecting means does not detect a data virus and for isolating the first data channel from the second data channel when the detecting means detects a data virus; and
  - e. means for decrypting data received from the first data channel and for encrypting data transmitted to first data channel.
2. An apparatus for isolating data receiving entity from a data sending entity, comprising:
  - a. a first data channel, coupled to the data sending entity;
  - b. a second data channel, coupled to the data receiving entity;
  - c. means, operatively coupled to the first data channel and to the second data channel, for decrypting data received from the first data channel and for encrypting data transmitted to first data channel;
  - d. means for comparing a plurality of data words received from the first data channel to at least one data word characteristic of a data virus and for asserting a control signal when a data word

received from the first data channel corresponds to a data word characteristic of a data virus; and

- e. means, coupled to the first data channel and the second data channel and operationally coupled to the control signal, for isolating the first data channel from the second data channel when the control signal is asserted and for placing the first data channel and the second data channel in optical communication when the control signal is not asserted.
- 3. The apparatus of Claim 2, wherein the comparing means comprises:
    - a. a processor; and
    - b. means for presenting to the processor at least one data word characteristic of a data virus.
  - 4. The apparatus of Claim 2, wherein the decrypting and encrypting means comprises a data encryption chip.
  - 5. The apparatus of Claim 3, wherein the processor comprises a screening environment processor.
  - 6. The apparatus of Claim 3, wherein the presenting means comprises a memory, operationally coupled to the processor, that stores at least one data word characteristic of a data virus.
  - 7. The apparatus of Claim 3, further comprising an input buffer that stores data received by the processor
  - 8. The apparatus of Claim 2, wherein data on the first data channel is transmitted in a serial format and wherein the apparatus further

comprises means for converting segments of serial data received from the first data channel to data in a parallel format.

9. The apparatus of Claim 2, wherein the isolating means comprises an optical isolator.
10. The apparatus of Claim 8, further comprising a controllable power supply responsive to the control signal from the comparing means, the power supply generating an enable signal when the control signal is not asserted, wherein the optical isolator is powered by the enable signal so that when the optical isolator receives power from the enable signal, the first data channel and the second data channel are in optical communication with each other.
11. An apparatus for isolating data receiving entity from a data sending entity, comprising:
  - a. a first data channel, coupled to the data sending entity;
  - b. a second data channel, coupled to the data receiving entity;
  - c. a data encryption chip, operatively coupled to the first data channel and to the second data channel, for decrypting data received from the first data channel and for encrypting data transmitted to first data channel;
  - d. a processor that is programmed to compare a plurality of data words received from the first data channel to at least one data word characteristic of a data virus and to assert a control signal when a data word received from the first data channel corresponds to a data word characteristic of a data virus;
  - e. a memory, operationally coupled to the processor, that stores at least one data word characteristic of a data virus that presents to

the processor at least one data word characteristic of a data virus;

- f. an input buffer that stores data received by the processor from the first data channel;
  - g. an optical isolator, coupled to the first data channel and the second data channel and having an enable signal input, that is capable of isolating the first data channel from the second data channel when the enable signal input is not asserted and is capable of placing the first data channel and the second data channel in optical communication with each other when the enable signal input is asserted; and
  - h. a controllable power supply responsive to the control signal from the processor and coupled to the enable signal input of the optical isolator, the power supply asserting the enable signal when the control signal is not asserted and the power supply not asserting the enable signal when the control signal is asserted, thereby causing the optical isolator to isolate the first data channel from the second data channel.
12. The apparatus of Claim 10, wherein the processor comprises a PCI host controller.
13. The apparatus of Claim 10, wherein data on the first data channel is transmitted in a serial format and wherein the apparatus further comprises means for converting segments of serial data received from the first data channel to data in a parallel format.
14. A method for isolating data receiving entity from a data sending entity, comprising:

- a. detecting a data virus received from the data sending entity;
- b. isolating the data sending entity from the data receiving entity upon detecting a data virus received from the data sending entity;
- c. decrypting data received from the data sending entity by the data receiving entity; and
- d. encrypting data sent from the data receiving entity to the data sending entity.

1/3

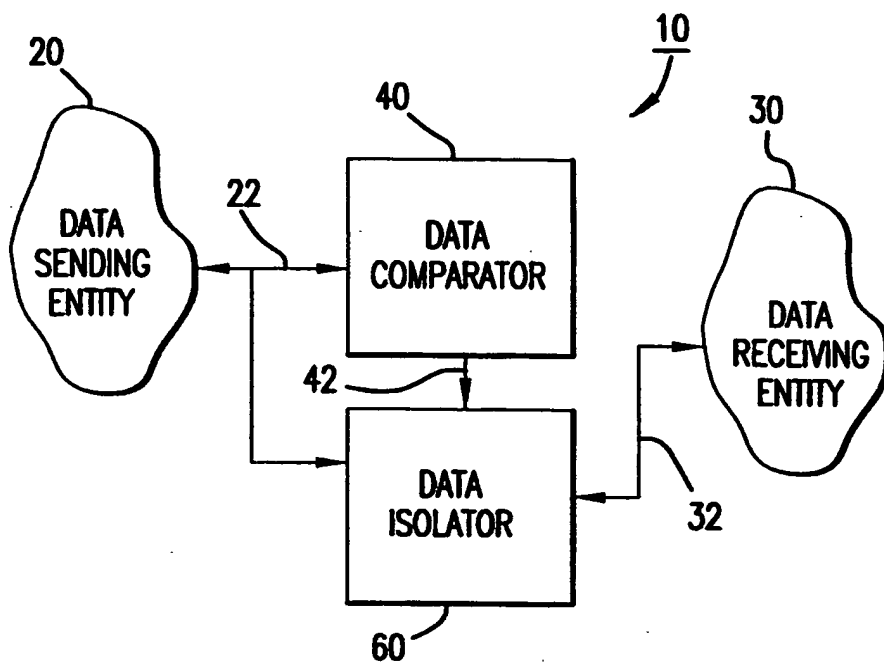
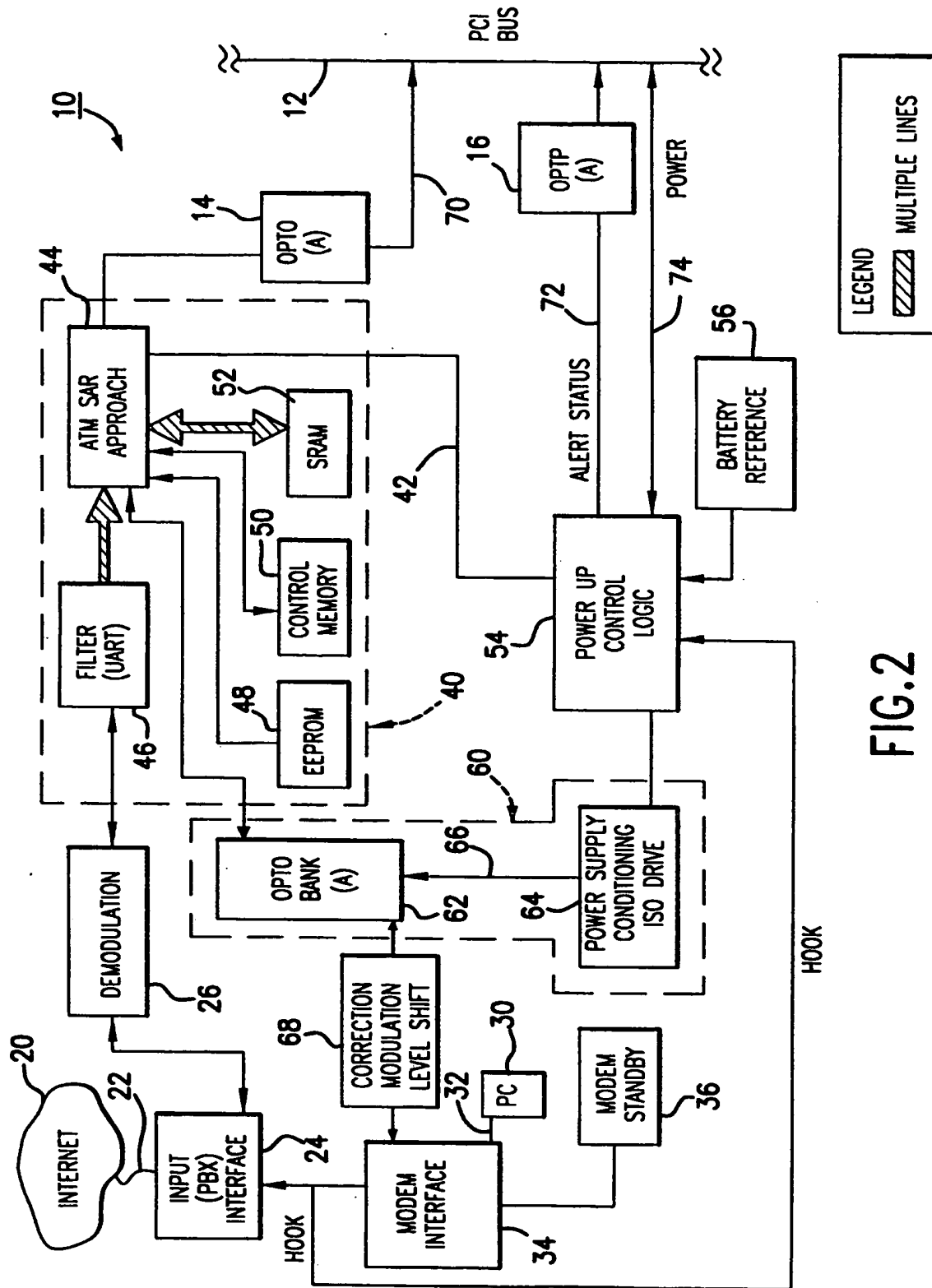
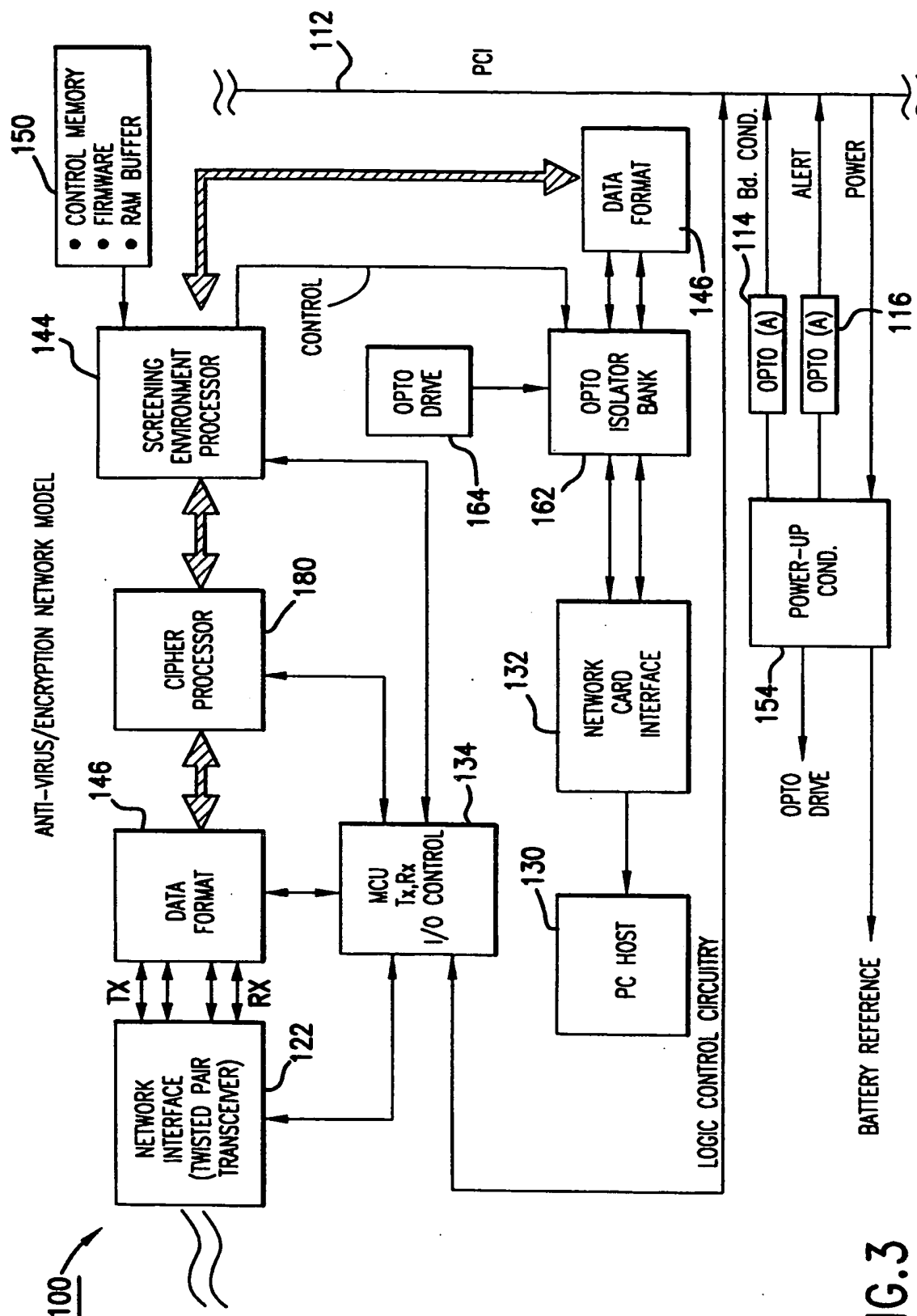


FIG.1



**FIG. 2**



**FIG. 3**

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/US98/25579

## A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : HD4L 12/22, 9/00

US CL : 395/187.01; 380/4, 49

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/4, 25, 49; 395/186, 187.01

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS: virus and network interface, optical isolator and PCI, data transmission; computer network and security and disconnect

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X — Y	US 5,414,833 A (HERSHEY et al) 09 MAY 1995, col. 16, lines 41-60.	1 and 14 2-13
Y	US 5,550,818 A (BRACKETT et al) 27 August 1996, col. 11, lines 1-30.	2-13
X — Y	US 5,434,562 A (REARDON) 18 July 1995, col. 3, line 28 through col. 4, line 8 and col. 4, line 63 through col. 5, line 31.	1 and 14. 2-13.
A	US 5,126,728 A (HALL) 30 June 1992, col. 7, lines 46-68.	1-14.



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"B" earlier document published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"A" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

28 JANUARY 1999

Date of mailing of the international search report

19 MAR 1999

Name and mailing address of the ISA/US  
Commissioner of Patents and Trademarks  
Box PCT  
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

GILBERTO BARRÓN JR.

Telephone No. (703) 305-1830